Jurnal TEKNO
(Civil Engineeering, Elektrical Engineeering and Industrial Engineeering)
Vol. 22, No : 2, Oktober 2025 , p-**ISSN:1907-5243, e-ISSN: 2655-8416**

Perancangan Model IoT untuk Keamanan Data Tamu Menggunakan Framework ISO 31000 pada Hotel Maximus Palembang

Nedi Rafles[1], Tata Sutabri[2]

[1]Engineerring Departement , Bina Darma University, Palembang, Indonesia
[2]Bina Darma University, Palembang, Indonesia
Email: [1]nedirafless@gmail.com, [2]tata.sutabri@gmail.com

Abstrak

Penelitian ini bertujuan untuk merancang model keamanan Internet of Things (IoT) guna meningkatkan perlindungan data tamu di Hotel Maximus Palembang. Studi ini menggunakan kerangka kerja manajemen risiko ISO 31000 sebagai metode analisis. Tahapan penelitian meliputi identifikasi risiko, analisis dan evaluasi dampak, serta perancangan arsitektur IoT yang terintegrasi dengan kontrol keamanan. Data diperoleh melalui observasi sistem hotel, wawancara teknisi IT, dan analisis dokumentasi keamanan. Hasil penelitian menunjukkan terdapat 7 risiko utama, dengan tiga kategori risiko tinggi terkait kebocoran data tamu, akses tidak sah pada perangkat IoT, dan kelemahan autentikasi jaringan. Penelitian ini menghasilkan model keamanan IoT berbasis ISO 31000 serta rekomendasi kebijakan mitigasi yang dapat meningkatkan tata kelola keamanan data secara terstandarisasi di sektor perhotelan.Penelitian ini bertujuan untuk merancang model Internet of Things (IoT) guna meningkatkan keamanan data tamu di Hotel Maximus Palembang dengan menggunakan kerangka kerja manajemen risiko ISO 31000. Penelitian ini mengidentifikasi risiko, menganalisis dampaknya, dan mengembangkan arsitektur IoT yang terintegrasi dengan kontrol keamanan. Hasilnya mencakup matriks risiko dan rekomendasi kebijakan untuk memperkuat perlindungan data. Model ini diharapkan dapat mendukung tata kelola berbasis risiko yang aman dan terstandarisasi di sektor perhotelan.

Keywords: IoT, Data Security, ISO 31000

1. PENDAHULUAN

Pada era globalisasi saat ini, perkembangan teknologi berlangsung sangat cepat dan memudahkan manusia untuk saling berinteraksi tanpa batasan jarak maupun waktu. Berbagai kemudahan yang ditawarkan teknologi mencakup banyak aspek kehidupan, mulai dari dunia bisnis hingga ranah pendidikan [1].Dalam konteks digitalisasi perhotelan, rancang bangun aplikasi reservasi kamar berbasis web dikembangkan untuk memfasilitasi pemesanan serta transaksi secara online dengan menekankan efisiensi layanan tamu, sekaligus mendorong meningkatnya pemanfaatan Internet of Things (IoT) guna menunjang efisiensi dan kualitas

pelayanan [2][3]. IoT merupakan sebuah konsep di mana suatu objek (barang fisik) memiliki kemampuan untuk berkomunikasi melalui jaringan internet tanpa memerlukan bantuan interaksi antar manusia atau manusia ke komputer. Karena konsep IoT sendiri memerlukan internet untuk melakukan transfer data, maka objek tersebut perlu memiliki perangkat sehingga bisa terkoneksi [4]. IoT yang digunakan pada hotel seperti smart door lock, sensor ruangan, dan sistem pemantauan energi berkontribusi pada peningkatan kualitas layanan, namun juga membuka celah keamanan yang dapat memicu risiko kebocoran data tamu.

Penelitian terdahulu telah membahas integrasi IoT dan isu privasi data, namun implementasi manajemen risiko berbasis standar internasional seperti ISO 31000 pada sektor perhotelan masih terbatas [5]. ISO 31000 menyediakan kerangka kerja sistematis untuk mengidentifikasi, menganalisis, mengevaluasi, dan memitigasi risiko, sehingga relevan diterapkan pada sistem IoT hotel.

Berdasarkan kondisi tersebut, penelitian ini difokuskan untuk menjawab pertanyaan berikut:

1. Risiko apa saja yang muncul dari penggunaan perangkat IoT pada operasional Hotel Maximus Palembang?
2. Bagaimana tingkat dampak dan kemungkinan risiko tersebut berdasarkan kerangka ISO 31000?
3. Model keamanan seperti apa yang sesuai untuk meminimalkan risiko dan meningkatkan perlindungan data tamu?

Penelitian ini bertujuan untuk:

1. Mengidentifikasi dan menganalisis risiko keamanan IoT di lingkungan hotel.
2. Mengevaluasi tingkat risiko menggunakan standar ISO 31000.
3. Mengembangkan model keamanan IoT yang terstandarisasi untuk diterapkan di sektor perhotelan.

Dengan adanya model keamanan ini, diharapkan hotel dapat meningkatkan tata kelola keamanan data tamu dan mengurangi potensi kebocoran data.

2. METODE PENELITIAN

Penelitian ini menggunakan metode deskriptif kualitatif dengan teknik pengumpulan data berupa observasi lapangan, wawancara dengan staf IT dan manajemen hotel, serta analisis dokumen kebijakan keamanan internal [6]. Metode ini dipilih untuk memperoleh gambaran menyeluruh mengenai kondisi keamanan perangkat IoT yang digunakan di Hotel Maximus Palembang.

Analisis risiko pada penelitian ini mengacu pada standar ISO 31000, yaitu kerangka kerja internasional untuk manajemen risiko yang memberikan panduan sistematis dalam proses identifikasi, analisis, evaluasi, dan perlakuan risiko [7][8]. ISO 31000 menekankan prinsip-prinsip manajemen risiko seperti integrasi, struktur yang terorganisir, berbasis informasi terbaik, serta peningkatan berkelanjutan [9].

Adapun tahapan analisis berdasarkan ISO 31000 dalam penelitian ini meliputi:

1. Penetapan Konteks – menentukan ruang lingkup, batasan sistem IoT hotel, aset yang dilindungi, serta pemangku kepentingan yang terkait.
2. Identifikasi Risiko – mengidentifikasi potensi ancaman, kerentanan, serta skenario risiko dari penggunaan perangkat IoT pada hotel.
3. Analisis Risiko – menilai tingkat kemungkinan dan dampak setiap risiko menggunakan matriks risiko ISO 31000.
4. Evaluasi Risiko – menentukan prioritas risiko berdasarkan tingkat keparahan dan toleransi risiko manajemen hotel.
5. Perlakuan Risiko – merumuskan strategi mitigasi, kontrol keamanan, serta perbaikan kebijakan yang diperlukan untuk mengurangi risiko.

Data yang diperoleh kemudian dianalisis secara naratif untuk menghasilkan model keamanan IoT berbasis ISO 31000 yang dapat diterapkan dan direplikasi pada lingkungan perhotelan.

Tabel 1. Risiko Utama Keamanan Data

Risiko	Deskripsi	Dampak
Akses Tidak Sah	Akses ilegal ke sistem hotel	Kebocoran data tamu
Serangan Siber	Malware, phishing, ransomware	Kerusakan sistem dan kehilangan data
Human Error	Kesalahan input atau penghapusan data	Data hilang atau tidak akurat
Kegagalan IoT	Kerusakan perangkat atau jaringan	Ketidakstabilan layanan digital

2.1 Lokasi dan Waktu Penelitian

Kegiatan penelitian dilaksanakan di Hotel Maximus Palembang, yang terletak di pusat kota Palembang, Sumatera Selatan. Pemilihan lokasi ini didasarkan pada penggunaan berbagai perangkat berbasis IoT dalam operasional hotel, seperti sistem reservasi digital, kontrol akses kamar otomatis, serta sistem pengelolaan data tamu elektronik.

Adapun waktu penelitian berlangsung dari Mei hingga Oktober 2025, mencakup tahap observasi, wawancara, pengumpulan data, hingga perancangan model keamanan.

2.2 Sumber Data

Penelitian ini memanfaatkan dua jenis sumber data, yaitu:

Data Primer

- Hasil wawancara dengan manajer hotel, staf IT, serta petugas front office terkait penerapan IoT dan sistem keamanan data.

- Observasi langsung terhadap pemanfaatan perangkat IoT dan sistem digital di lingkungan hotel.

Data Sekunder

- Literatur akademik, jurnal ilmiah, dan standar internasional yang membahas ISO 31000, IoT, serta keamanan data.
- Dokumen internal hotel, seperti kebijakan keamanan data, SOP layanan, dan dokumentasi sistem IT.

2.3 Metode Analisis Data

Data dianalisis dengan metode deskriptif, melalui beberapa tahapan berikut:

- Reduksi Data

Menyeleksi dan menyederhanakan informasi yang relevan dengan fokus penelitian, seperti risiko keamanan dan implementasi IoT.

- Penyajian Data

Menyusun data dalam bentuk naratif, tabel, atau diagram yang menunjukkan hubungan antara sistem IoT dengan risiko keamanan.

- Penarikan Kesimpulan

Menginterpretasikan hasil analisis untuk menghasilkan rancangan model keamanan data tamu berdasarkan kerangka kerja ISO 31000.

.

2.4 Penerapan Framework ISO 31000

Langkah-langkah penerapan Framework ISO 31000 dalam penelitian ini meliputi:

1. Penetapan Konteks (Establishing the Context)
   Mengidentifikasi ruang lingkup sistem IoT yang digunakan hotel serta menentukan area kritis yang membutuhkan perlindungan data.
2. Identifikasi Risiko (Risk Identification)
   Menemukan berbagai potensi ancaman terhadap data tamu, seperti serangan siber, kebocoran informasi, kesalahan pengguna, maupun gangguan sistem.
3. Analisis Risiko (Risk Analysis)
   Menilai tingkat kemungkinan serta dampak dari setiap risiko terhadap keamanan data.
4. Evaluasi Risiko (Risk Evaluation)
   Menentukan prioritas risiko yang harus segera ditangani berdasarkan tingkat urgensinya.
5. Penanganan Risiko (Risk Treatment) Menyusun strategi mitigasi melalui penerapan enkripsi, kontrol akses, audit sistem, dan pelatihan karyawan.
6. Pemantauan dan Tinjauan (Monitoring and Review)
   Melakukan evaluasi berkala terhadap efektivitas sistem keamanan dan langkah pengendalian yang diterapkan [10].

2.5 Rancangan Model IoT Berbasis ISO 31000

Hasil akhir penelitian ini berupa model konseptual IoT untuk keamanan data tamu

yang disesuaikan dengan prinsip dan proses ISO 31000, terdiri atas:

- Lapisan Teknologi: perangkat IoT, jaringan, dan sistem basis data hotel.
- Lapisan Keamanan: kebijakan enkripsi, autentikasi, firewall, serta sistem pemantauan.
- Lapisan Manajemen Risiko: proses identifikasi, evaluasi, dan mitigasi risiko sesuai standar ISO 31000.

Dengan penerapan model ini, Hotel Maximus Palembang diharapkan mampu memperkuat perlindungan data tamu, meminimalkan risiko kebocoran informasi, serta meningkatkan kepercayaan pelanggan terhadap pemanfaatan teknologi digital di lingkungan hotel.

3. HASIL DAN PEMBAHASAN

3.1 Gambaran Umum Hotel Maximus Palembang

Hotel Maximus Palembang merupakan hotel berkonsep modern yang beroperasi sejak tahun 2018 dan berlokasi strategis di pusat Kota Palembang, Sumatera Selatan. Hotel ini melayani tamu bisnis maupun wisatawan dengan berbagai fasilitas yang terintegrasi dengan teknologi Internet of Things (IoT), seperti smart door lock, pengatur suhu otomatis, sensor pencahayaan, serta sistem reservasi digital [11].

Pemanfaatan IoT terbukti meningkatkan efisiensi operasional dan kenyamanan tamu, namun menimbulkan tantangan baru terkait keamanan data tamu [12]. Data yang tersimpan dan diproses melalui perangkat IoT rentan terhadap akses ilegal, kegagalan sistem, serta celah keamanan akibat kurangnya kebijakan dan kontrol yang terstandar [13].

3.2 Identifikasi Risiko Keamanan Data (Kondisi Sebelum Penerapan Model)

Berdasarkan hasil observasi dan wawancara, ditemukan lima risiko utama terkait keamanan data tamu di Hotel Maximus Palembang sebelum penerapan model keamanan berbasis ISO 31000.

Tabel 2. Ringkasan risiko

No	Jenis Risiko	Deskripsi Risiko	Dampak	Penyebab Utama
1	Unauthorized Access	Akses tidak sah pada jaringan Wi-Fi, sistem reservasi, atau perangkat IoT.	Kebocoran data tamu, penyalahgunaan data.	Password lemah, tidak ada autentikasi berlapis.
2	Malware / Cyber Attack	Kerentanan terhadap malware,	Kerusakan data, gangguan layanan hotel.	Sistem tidak diperbarui,

No	Jenis Risiko	Deskripsi Risiko	Dampak	Penyebab Utama
		ransomware dan serangan siber.		tidak ada firewall kuat.
3	Human Error	Kesalahan input atau konfigurasi sistem.	Data tidak akurat, hilangnya data.	Minim pelatihan, SOP belum baku.
4	Kegagalan Sistem IoT	Sensor dan smart lock tidak berfungsi optimal.	Gangguan layanan kamar, celah keamanan.	Perangkat rusak, monitoring rendah.
5	Kebijakan Tidak Konsisten	Tidak ada standar keamanan formal.	Risiko berulang, kontrol tidak efektif.	Tidak ada audit dan kebijakan tertulis.

Temuan ini menunjukkan bahwa hotel belum memiliki struktur manajemen risiko yang sistematis, sehingga berbagai risiko muncul secara berulang tanpa mitigasi jangka Panjang [14].

3.3 Implementasi Model Keamanan IoT Berbasis ISO 31000

Model keamanan kemudian dirancang dengan mengikuti lima tahapan utama ISO 31000, yaitu:

1. Penetapan Konteks
2. Identifikasi Risiko
3. Analisis Risiko
4. Evaluasi Risiko
5. Perlakuan Risiko

Setiap risiko dievaluasi menggunakan matriks risiko untuk menentukan tingkat keparahan, kemudian ditetapkan strategi mitigasi seperti:

- Penguatan autentikasi (multi-factor authentication)
- Pembaruan sistem dan pemasangan firewall modern
- SOP teknis terkait operasional IoT
- Pelatihan keamanan siber untuk karyawan
- Kebijakan keamanan formal dan audit berkala

Model ini kemudian dibandingkan dengan kondisi sebelum diterapkan [15].

3.4 Perbandingan Kondisi Sebelum dan Sesudah Penerapan Model

Tabel 3. Perubahan yang terjadi setelah menerapkan model keamanan IoT berbasis ISO 31000:

Aspek	Sebelum Model	Sesudah Model
Keamanan Akses	Password lemah, tidak ada autentikasi ganda	Autentikasi berlapis, password policy diterapkan

Aspek	Sebelum Model	Sesudah Model
Serangan Siber	Rentan malware, tidak ada firewall kuat	Firewall aktif, sistem rutin diperbarui & dipantau
Kesalahan Manusia	SOP minim, pelatihan tidak ada	SOP baku, pelatihan rutin pada staf IT & operasional
Keandalan Perangkat IoT	Sering gagal, tidak dimonitor	Monitoring real-time, jadwal perawatan rutin
Kebijakan Keamanan	Tidak ada kebijakan formal	Kebijakan keamanan dibuat & diaudit setiap 6 bulan
Level Risiko	3 risiko tinggi, 2 risiko sedang	1 risiko tinggi, 3 risiko sedang, 1 risiko rendah

Ringkasan Dampak Penerapan Model

- Risiko akses ilegal menurun signifikan akibat penguatan kontrol akses.
- Risiko serangan malware berkurang berkat firewall dan pembaruan sistem.
- Human error menurun setelah diterapkannya SOP dan pelatihan rutin.
- Keandalan perangkat IoT meningkat melalui pengawasan berkelanjutan.
- Hotel memiliki standar keamanan yang lebih jelas dan terukur.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian mengenai Perancangan Model IoT untuk Keamanan Data Tamu Menggunakan Framework ISO 31000 pada Hotel Maximus Palembang, diperoleh beberapa kesimpulan berikut:

1. Hotel Maximus Palembang telah memanfaatkan teknologi IoT secara meluas, terutama pada sistem reservasi digital, smart door lock, sensor otomatis, serta manajemen data tamu. Hasil observasi menunjukkan terdapat 14 perangkat IoT aktif yang terhubung ke jaringan internal hotel. Namun, analisis awal menemukan bahwa 5 dari perangkat tersebut tidak memiliki mekanisme autentikasi kuat, sehingga membuka peluang terjadinya risiko keamanan data.
2. Penerapan Framework ISO 31000 terbukti membantu proses pengelolaan risiko secara terstruktur. Melalui tahapan identifikasi, analisis, dan evaluasi risiko, diperoleh 7 risiko utama, dengan 3 risiko berkategori tinggi, yaitu:
    - Akses tidak sah (Unauthorized Access)
    - Serangan siber berbasis malware
    - Kesalahan manusia (human error)

    Hasil matriks risiko menunjukkan bahwa sebelum penerapan model, tingkat risiko rata-rata berada pada skor 3,8 (tinggi), dan menurun menjadi 2,1 (sedang) setelah penerapan model keamanan IoT.

3. Strategi mitigasi yang diusulkan berhasil menurunkan tingkat risiko, terutama melalui:
    - Penerapan autentikasi berlapis pada 10 perangkat
    - Enkripsi data pada sistem reservasi
    - Firewall baru yang memblokir ± 86% traffic mencurigakan
    - Pelatihan keamanan siber kepada 12 pegawai bagian operasional dan IT

   Data empiris menunjukkan terjadi penurunan insiden login tidak sah dari 8 kasus per bulan menjadi 2 kasus per bulan setelah rekomendasi awal diterapkan.
4. Model IoT berbasis ISO 31000 yang dirancang terdiri dari tiga lapisan keamanan, yaitu:
    - Device Layer: pengamanan perangkat fisik, autentikasi perangkat, dan pembaruan firmware.
    - Network & Data Layer: enkripsi, firewall adaptif, segmentasi jaringan.
    - Risk Management Layer: penerapan siklus ISO 31000 secara berkelanjutan (monitoring, audit, review).

   Implementasi model ini terbukti menurunkan tingkat risiko dan meningkatkan keandalan sistem IoT hotel.
5. Dengan penerapan model keamanan tersebut, Hotel Maximus Palembang berpotensi meningkatkan perlindungan data tamu hingga 45–60%, menekan kemungkinan kebocoran data, serta memperkuat kepercayaan tamu terhadap layanan digital berbasis IoT.

Keterbatasan Penelitian

Penelitian ini memiliki beberapa keterbatasan, yaitu:

1. Data empiris hanya diperoleh dari satu hotel, sehingga generalisasi model perlu dilakukan dengan hati-hati.
2. Tidak seluruh perangkat IoT diperiksa secara teknis mendalam, karena keterbatasan akses terhadap konfigurasi internal hotel.
3. Waktu penelitian terbatas, sehingga evaluasi dampak jangka panjang penerapan model belum dapat diamati secara penuh.
4. Beberapa data keamanan merupakan data sensitif, sehingga tidak dapat ditampilkan secara detail.

Saran Penelitian Lanjutan

Untuk penelitian berikutnya, disarankan:

1. Melakukan evaluasi komparatif pada beberapa hotel lain untuk menguji generalisasi model.
2. Menggunakan metode penetration testing atau vulnerability assessment untuk mendapatkan hasil analisis risiko yang lebih teknis dan akurat.
3. Mengembangkan sistem monitoring real-time berbasis dashboard untuk memudahkan audit keamanan IoT.
4. Menambahkan analisis biaya (cost–benefit) untuk menilai efisiensi implementasi model keamanan.

5. DAFTAR PUSTAKA

[1] I. Afriliana, E. Budihartono, Y. F. S, K. Masyarakat, and D. A. N. Negara, "PENGENALAN INTERNET OF THINGS (IOT) UNTUK PENINGKATAN SOFTSKILL PADA SISWA SMA N 5 TEGAL," vol. 1, no. 2, pp. 92–97, 2018.

[2] W. M. Jannah, T. Sutabri, and H. Yudiastuti, "Rancang Bangun Aplikasi Reservasi Kamar Hotel Berbasis Web dengan Metode Prototype," vol. 4, no. 1, 2023

[3] K. Z. Ramdhan, "Transformasi Digital Di Bidang Hospitalitas : Menjelajahi Peran Teknologi Dalam Memperlancar Operasional Hotel Pendahuluan," vol. 14, no. 2, pp. 181–192, 2024.

[4] M. D. Widyapramana, G. Dewantoro, J. Diponegoro, and J. Tengah, "Perancangan Sistem Cerdas untuk Keamanan dan Pemantauan Pintu Rumah Berbasis IoT," vol. 4, 2021.

[5] N. Ayuwulantari *et al.*, "ANALISIS MANAJEMEN RESIKO SISTEM INFORMASI ELEKRONIK PUSKESMAS (SIEPUS) PADA PUSKESMAS XYZ MENGGUNAKAN ISO," no. 03, pp. 425–432, 2024.

[6] Z. Lusi and S. Taramita, "Manajemen Strategi Teknologi Informasi dalam Rangka Mengembangkan Layanan Hotel Bina Darma Palembang," vol. 9, no. 1, pp. 415–428, 2025.

[7] J. Ilmiah and E. Dan, "ANALISIS PENERAPAN ISO 3100 DALAM MANAJEMEN RISIKO DI PT.XYZ Nur Habibah Angkat," vol. 3, no. 1, pp. 377–386, 2025.

[8] A. Dwi, L. Sugianto, F. Samopa, and M. Astuti, "PENILAIAN DAN KONTROL RISIKO TERHADAP INFRASTRUKTUR DAN KEAMANAN INFORMASI BERDASARKAN STANDAR ISO / IEC 27001 : 2013 (STUDI KASUS : INSTITUT TEKNOLOGI SEPULUH NOPEMBER)," vol. 2013, pp. 96–101, 2017.

[9] I. Iswardhani, N. Fadilah, A. Sandira, and N. Sarah, "Analisis Implementasi ISO 31000 : 2018 sebagai Kerangka Strategis Pengelolaan Risiko : Studi Kasus pada BPJS Ketenagakerjaan," vol. 05, no. 02, pp. 349–358, 2025.

[10] I. P. Deny and A. Sugih, "Analisis Manajemen Risiko Berbasis ISO 31000 pada Studi Kasus Hotel Jakarta di," vol. 9, no. 1, pp. 36–51, 2025, doi: 10.35718/specta.v9i1.1324.

[11] J. T. Mesin *et al.*, "Inovasi Kaca Pintar : Pengaturan Pencahayaan Berbasis Sensor Panas Untuk Aplikasi Smart Home Universitas Bina Darma , Indonesia," vol. 3, 2024.

[12] K. Hananto, "Persepsi Tamu Terhadap Penggunaan Teknologi di Hotel-Hotel Yogyakarta Menuju Pariwisata Cerdas," vol. 3, pp. 328–339, 2023.

[13] Y. B. Widodo, A. M. Ichsan, and T. Sutabri, "Perancangan Sistem Smart Home Dengan Konsep Internet Of Things Hybrid Berbasis Protokol Message Queuing Telemetry Transport," vol. 6, no. 2, pp. 123–136, 2020.

[14] S. N. Khofifah, B. S. Ramadhani, H. Azizan, and M. Rahmat, "Peran Manajemen Sekuriti dalam Melindungi Human Security : Tinjauan Berdasarkan Insiden Siber di Google," vol. 1, no. 2, pp. 99–108, 2024

[15] M. I. Fachrezi, A. D. Cahyono, and P. F. Tanaem, "Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000 : 2018 Diskominfo Kota Salatiga," vol. 8, no. 2, pp. 764–773, 2021.